Weekly Report

1 Done

1.1 Paper Review

This is not a satisfied paper for its incomplete article structure and simple designs. The comments have been sent by email.

1.2 MOOC courses

I read the related chapter in the new textbook and summarized four subsections for MOOC courses.

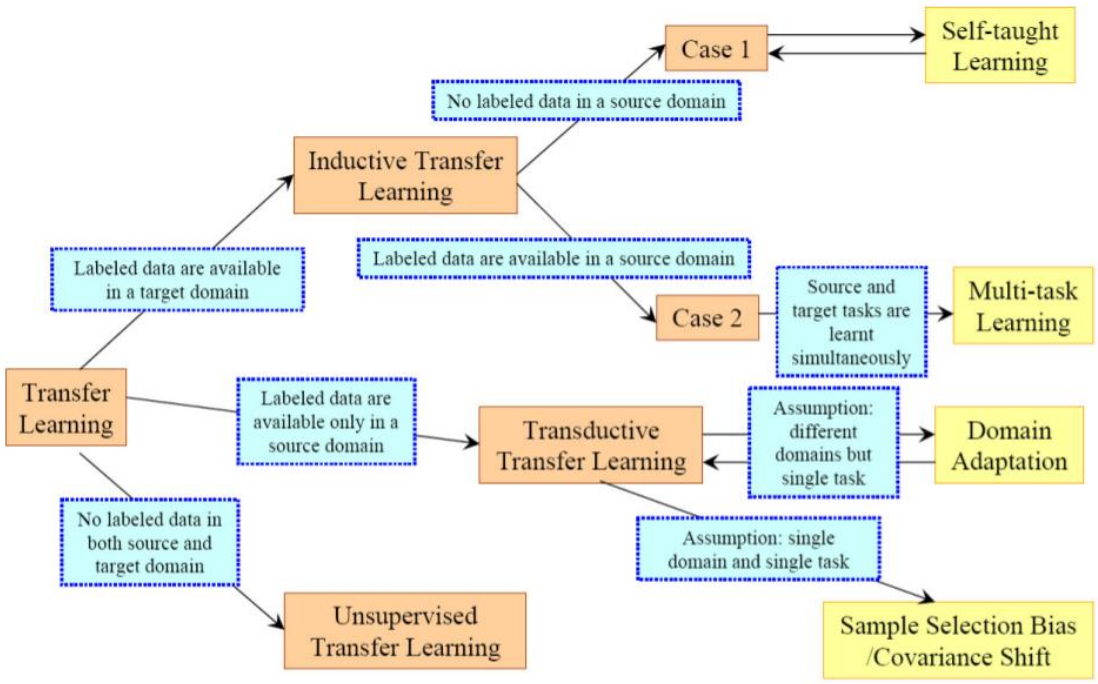
1.3 Event Sequence Prediction

I Implemented the clustering function.

1.4 Federated Learning

- Learn about transfer learning.
  - https://github.com/jindongwang/transferlearning#1introduction-and-tutorials-%E7%AE%80%E4%BB%8B%E4%B8%8E%E6%95%99%E7%A8%8B
  - "A Survey on Transfer Learning"

Learning Settings		Source and Target Domains	Source and Target Tasks
Traditional Machine Learning		the same	the same
Transfer Learning	*Inductive Transfer Learning* / *Unsupervised Transfer Learning*	the same	different but related
		different but related	different but related
	Transductive Transfer Learning	different but related	the same



- Read paper and materials about the federated learning.

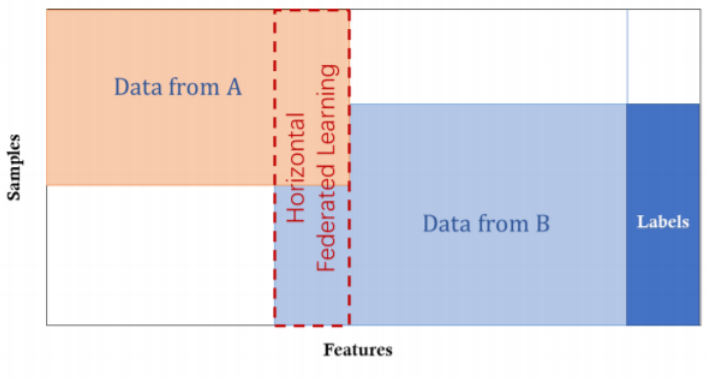
- I followed the blog of federated learning on WeChat.
- "Federated Machine Learning: Concept and Applications"

2.1 Definition of Federated Learning

Define N data owners $\{\mathcal{F}_1, ...\mathcal{F}_N\}$, all of whom wish to train a machine learning model by consolidating their respective data $\{\mathcal{D}_1, ...\mathcal{D}_N\}$. A conventional method is to put all data together and use $\mathcal{D} = \mathcal{D}_1 \cup ... \cup \mathcal{D}_N$ to train a model $\mathcal{M}_{SUM}$. A federated learning system is a learning process in which the data owners collaboratively train a model $\mathcal{M}_{FED}$, in which process any data owner $\mathcal{F}_i$ does not expose its data $\mathcal{D}_i$ to others [1]. In addition, the accuracy of $\mathcal{M}_{FED}$, denoted as $\mathcal{V}_{FED}$ should be very close to the performance of $\mathcal{M}_{SUM}$, $\mathcal{V}_{SUM}$. Formally, let δ be a non-negative real number, if

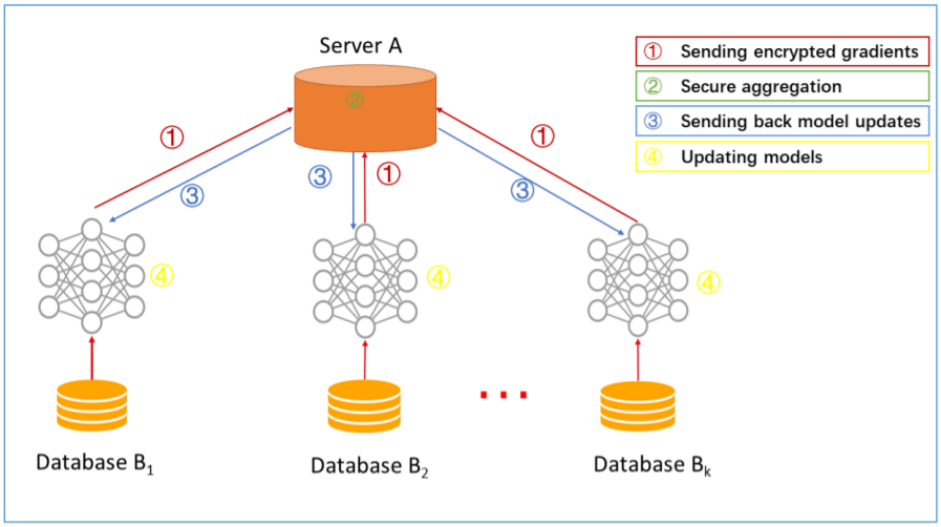
$$| \mathcal{V}_{FED} - \mathcal{V}_{SUM} | < \delta \tag{1}$$

we say the federated learning algorithm has δ-accuracy loss.

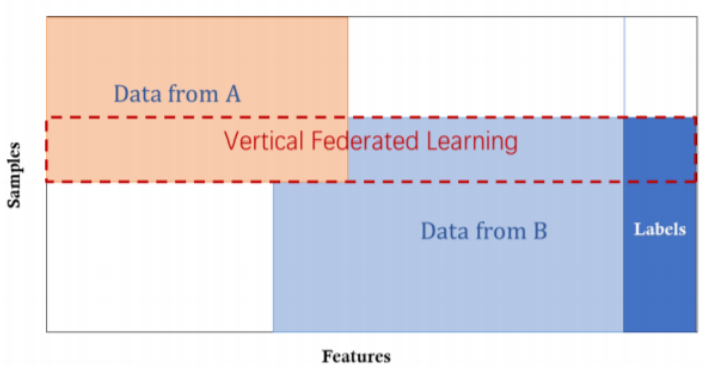


(a) Horizontal Federated Learning

Architecture for a horizontal federated learning system.

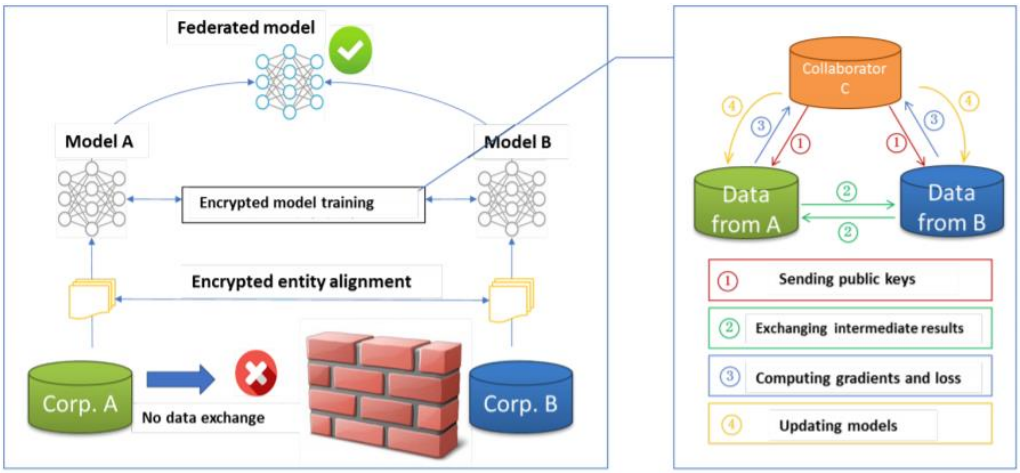


1) Participants locally compute training gradients, mask a selection of gradients with encryption, differential privacy or secret sharing techniques, and send masked results to server;
2) Server performs secure aggregation without learning information about any participant;
3) Server send back the aggregated results to participants;
4) Participants update their respective model with the decrypted gradients.



(b) Vertical Federated Learning

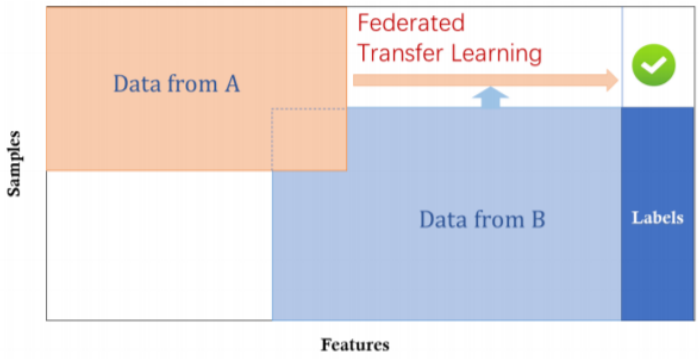
Architecture for a vertical federated learning system.



1) Collaborator C creates encryption pairs, send public key to A and B;
2) A and B encrypt and exchange the intermediate results for gradient and loss calculations;
3) A and B computes encrypted gradients and adds additional mask, respectively, and B also computes encrypted loss; A and B send encrypted values to C;
4) C decrypts and send the decrypted gradients and loss back to A and B; A and B unmask the gradients, update the model parameters accordingly.

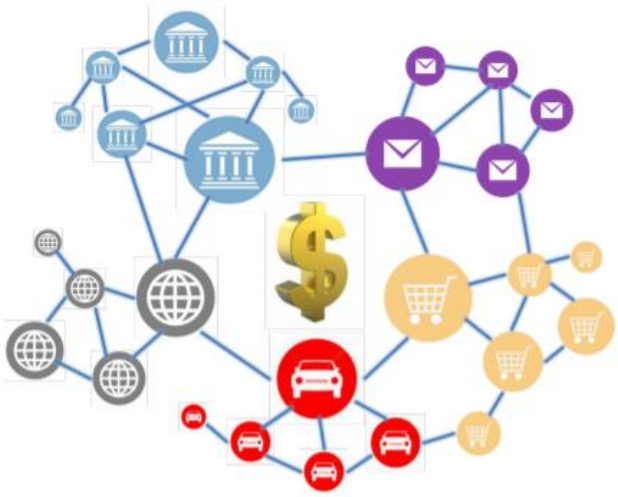
Ex. Linear Regression

	party A	party B	party C
step 1	initialize Θ_A	initialize Θ_B	create an encryption key pair, send public key to A and B;
step 2	compute $[[u_i^A]],[[\mathcal{L}_A]]$ and send to B;	compute $[[u_i^B]],[[d_i^B]],[[\mathcal{L}]]$, send $[[d_i^B]]$ to A, send $[[\mathcal{L}]]$ to C;	
step 3	initialize R_A, compute $[[\frac{\partial \mathcal{L}}{\partial \Theta_A}]]+[[R_A]]$ and send to C;	initialize R_B, compute $[[\frac{\partial \mathcal{L}}{\partial \Theta_B}]]+[[R_B]]$ and send to C;	C decrypt $\mathcal{L}$, send $\frac{\partial \mathcal{L}}{\partial \Theta_A}+R_A$ to A, $\frac{\partial \mathcal{L}}{\partial \Theta_B}+R_B$ to B;
step 4	update Θ_A	update Θ_B	
what is obtained	Θ_A	Θ_B	



(c) Federated Transfer Learning

- Applications:



It can establish a united model for multiple enterprises while the local data is protected. For example, when predicting customers' preferences, it can take benefits from both purchasing power from bank information and product characteristics from retail datasets.

- Configured the environment for federated learning based on TensorFlow and run the code provided by official website.

2 To Do

- Making slides for MOOC.

- Understand the algorithms and the code of federated learning.